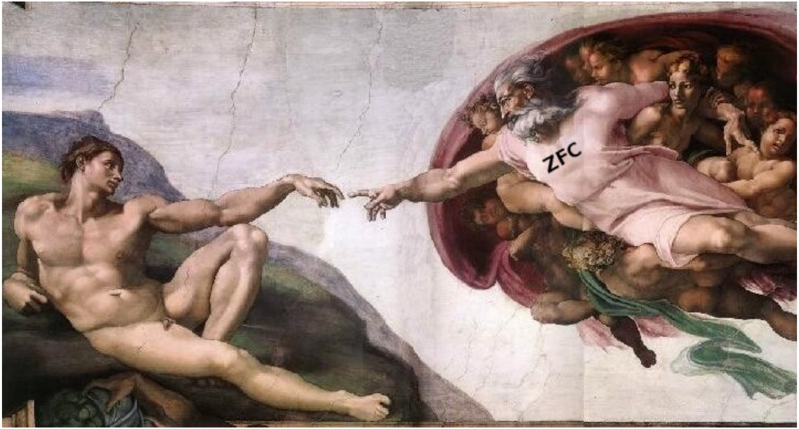
Introduction aux

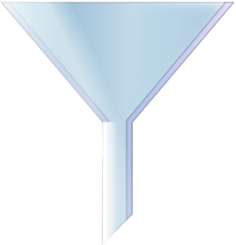
Mathématiques à rebours

Ludovic PATEY

9 octobre 2017


ZFC

Mathématiques infinitaires



PRA

Théorème

$$T$$

Axiomes Théorème

$$A_1, \ldots, A_n \Rightarrow T$$

Axiomes		Théorème
$A_1, \ldots, A_n$	$\Leftarrow$	T

Arithmétique du second ordre

$$t ::= 0 \mid 1 \mid x \mid t_1 + t_2 \mid t_1 \cdot t_2$$

$$\begin{aligned} f ::= \; & t_1 = t_2 \mid t_1 < t_2 \mid t_1 \in X \mid f_1 \vee f_2 \\ & \mid \neg f \mid \forall x.f \mid \exists x.f \mid \forall X.f \mid \exists X.f \end{aligned}$$

(Hilbert et Bernays)

Un ensemble $A \subseteq \mathbb{N}$ est calculable s'il existe un programme informatique qui, pour une entrée n, décide si $n \in A$.

Thèse de Church-Turing

Cette définition est indépendante du langage de programmation choisi.

Arithmétique de Robinson

1. $m + 0 = m$
2. $m + (n + 1) = (m + n) + 1$
3. $m \times 0 = 0$
4. $m \times (n + 1) = (m \times n) + m$
5. $m + 1 \neq 0$
6. $m + 1 = n + 1 \rightarrow m = n$
7. $\neg(m < 0)$
8. $m < n + 1 \leftrightarrow (m < n \vee m = n)$

Schéma de compréhension

$$\exists X \forall n (n \in X \Leftrightarrow \varphi(n))$$

pour toute formule $\varphi(n)$ où X est libre.

Hiérarchie arithmétique

- Σ^0_1 : définissable par une formule $\exists n.\phi$
- Π^0_1 : définissable par une formule $\forall n.\phi$
- Δ^0_1 : à la fois Σ^0_1 et Π^0_1

où ϕ est une formule ne contenant que des quantificateurs bornés.

Hiérarchie arithmétique

- Σ^0_1 : définissable par une formule $\exists n.\phi$
- Π^0_1 : définissable par une formule $\forall n.\phi$
- Δ^0_1 : à la fois Σ^0_1 et Π^0_1

où ϕ est une formule ne contenant que des quantificateurs bornés.

Calculable = définissable par un prédicat Δ^0_1

Schéma de **compréhension** Δ^0_1

$$\forall n(\varphi(n) \Leftrightarrow \psi(n)) \Rightarrow \exists X \forall n(n \in X \Leftrightarrow \varphi(n))$$

où $\varphi(n)$ est une formule Σ^0_1 où X est libre, et ψ est une formule Π^0_1.

Schéma d'induction

$$\varphi(0) \wedge \forall n(\varphi(n) \Rightarrow \varphi(n+1)) \Rightarrow \forall n \varphi(n)$$

pour toute formule $\varphi(n)$

Schéma d'induction Σ^0_1

$$\varphi(0) \wedge \forall n(\varphi(n) \Rightarrow \varphi(n+1)) \Rightarrow \forall n \varphi(n)$$

où $\varphi(n)$ est une formule Σ^0_1

équivalent à

Schéma de compréhension bornée Σ^0_1

$$\forall p \exists X \forall n(n \in X \Leftrightarrow n < p \wedge \varphi(n))$$

où $\varphi(n)$ est une formule Σ^0_1 où X est libre.

Schéma d'induction Σ^0_1

$$\varphi(0) \wedge \forall n(\varphi(n) \Rightarrow \varphi(n+1)) \Rightarrow \forall n \varphi(n)$$

où $\varphi(n)$ est une formule Σ^0_1

RCA_0

Arithmétique de Robinson

$$m+1 \neq 0$$
$$m+1 = n+1 \rightarrow m = n$$
$$\neg(m < 0)$$
$$m < n+1 \leftrightarrow (m < n \vee m = n)$$

$$m+0 = m$$
$$m+(n+1) = (m+n)+1$$
$$m \times 0 = 0$$
$$m \times (n+1) = (m \times n)+m$$

Schéma d'induction Σ_1^0

$$\varphi(0) \wedge \forall n(\varphi(n) \Rightarrow \varphi(n+1))$$
$$\Rightarrow \forall n \varphi(n)$$

où $\varphi(n)$ est une formule Σ_1^0

Schéma de compréhension Δ_1^0

$$\forall n(\varphi(n) \Leftrightarrow \psi(n))$$
$$\Rightarrow \exists X \forall n(n \in X \Leftrightarrow \varphi(n))$$

où $\varphi(n)$ est une formule Σ_1^0 où X est libre, et ψ est une formule Π_1^0.

RCA_0 capture les mathématiques calculables

$$\mathcal{M} = (\omega, \{X : X \text{ calculable }\}, +, \cdot <)$$

Les mathématiques sont calculatoirement très structurées

Presque tous les théorèmes sont empiriquement équivalents à un parmi cinq ensembles d'axiomes.

$$\begin{array}{c} \Pi^1_1\mathsf{CA} \\ \downarrow \\ \mathsf{ATR} \\ \downarrow \\ \mathsf{ACA} \\ \downarrow \\ \mathsf{WKL} \\ \downarrow \\ \mathsf{RCA}_0 \end{array}$$

Enoncés équivalents à WKL

- Le lemme de couverture de Heine/Borel : Toute couverture de l'intervalle $[0,1]$ par une séquence d'ouverts admet une sous-couverture finie.
- Toute fonction à valeurs réelles sur $[0,1]$ est bornée.
- Le théorème de complétude de Gödel : tout ensemble dénombrable d'énoncés dans le calcul des prédicats admet un modèle dénombrable.
- Tout anneau commutatif dénombrable admet un idéal premier.
- Tout corps dénombrable de caractéristique 0 admet une unique cloture algébrique
- Le théorème de point fixe de Brouwer : Toute fonction uniformément continue sur $[0,1]^n$ admet un point fixe.

Enoncés équivalents à ACA

- Toute suite de réels croissante bornée a un supremum.
- Le théorème de Bolzano/Weierstrass : Toute suite de réels a une sous-suite convergente.
- Tout anneau commutatif dénombrable a un idéal maximal.
- Tout espace vectoriel sur $\mathbb{Q}$ admet une base.
- Tout corps dénombrable de caractéristique 0 a une base de transcendance.
- Le lemme de König : Tout arbre infini à branchement fini admet un chemin infini.
- Le théorème de Ramsey pour les coloriages de $[\mathbb{N}]^3$.

ENONCÉS ÉQUIVALENTS À ATR

- Toute paire d'ordres bien-fondés dénombrables est comparables.
- Le théorème d'Ulm : Les *p*-groupes abéliens réduits dénombrables ayant les mêmes invariants d'Ulm sont isomorphes.
- Le théorème de séparation de Lusin : toute paire d'ensembles analytiques disjoints peut être séparée par un ensemble borélien.
- Tout sous-ensemble ouvert de $[\mathbb{N}]^{\mathbb{N}}$ a la propriété de Ramsey.

ENONCÉS ÉQUIVALENTS À Π^1_1CA

- Tout arbre a un sous-arbre parfait maximal.
- Le théorème de Cantor/Bendixson : Tout sous-ensemble fermé de $\mathbb{R}$ est l'union d'un ensemble dénombrable et d'un ensemble parfait.
- Tout groupe abélien dénombrable est la somme directe d'un groupe divisible et d'un groupe réduit.
- Tout ensemble G_δ a la propriété de Ramsey.

PROGRAMME DE HILBERT

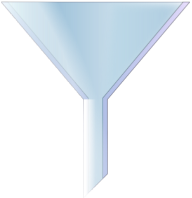
Justification des méthodes infinitaires pour prouver le fini

Réductionnisme finitaire :

$$T \vdash \varphi \Rightarrow PRA \vdash \varphi$$

pour φ une formule Π^0_1

"Au moins 85% des mathématiques sont réductibles à des méthodes finitaires"
(Stephen Simpson)



THÉORÈME DE RAMSEY

$[X]^n$ est l'ensemble des n-uplets non-ordonnés dans X

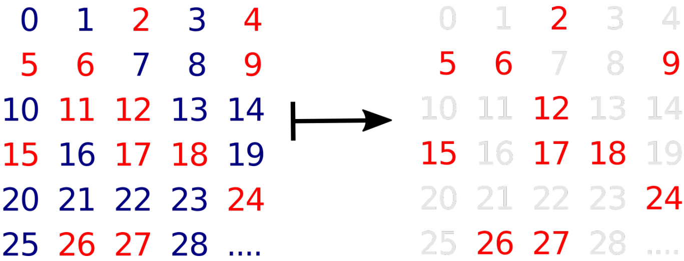
Un k-coloriage de $[X]^n$ est une fonction $f : [X]^n \to k$

Un ensemble $H \subseteq X$ est homogène pour f si $|f([H]^n)| = 1$.

RT^n_k Tout k-coloriage de $[\mathbb{N}]^n$ admet un ensemble homogène infini.

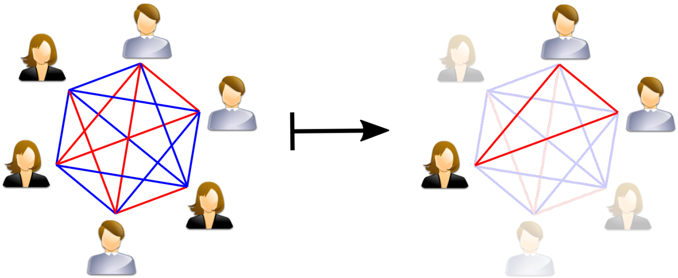
PRINCIPE DES TIROIRS

RT^1_k Toute k-partition de $\mathbb{N}$ admet une partie infinie.



Théorème de Ramsey pour les paires

RT^2_k Tout k-coloriage d'une clique infinie admet une sous-clique infinie monochromatique.



Les mathématiques sont calculatoirement très structurées

Presque tous les théorèmes sont empiriquement équivalents à un parmi cinq ensembles d'axiomes.

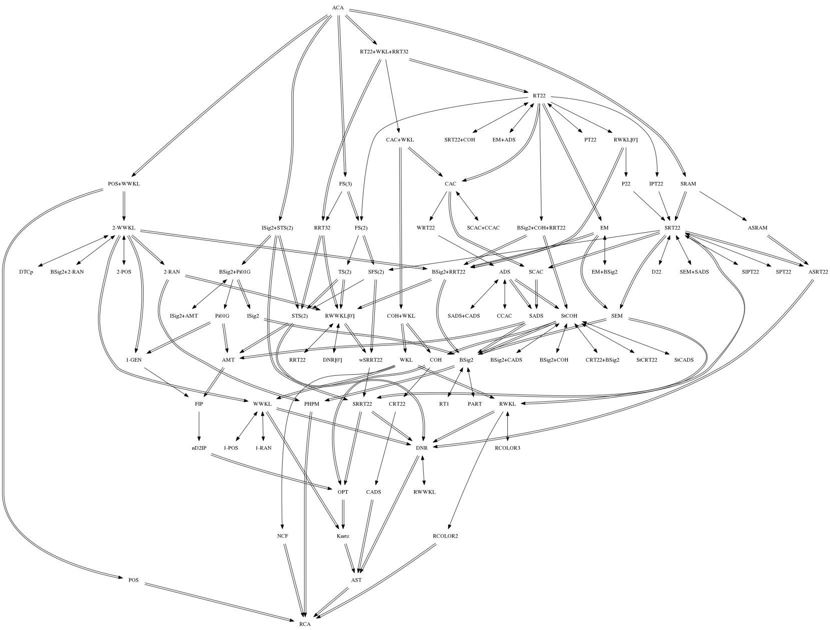
$$\Pi^1_1\mathsf{CA} \downarrow \mathsf{ATR} \downarrow \mathsf{ACA} \downarrow \mathsf{WKL} \downarrow \mathsf{RCA}_0$$

Les mathématiques sont calculatoirement très structurées

$$
\begin{tikzcd}
 & \Pi^1_1\mathsf{CA} \arrow[d] \\
 & \mathsf{ATR} \arrow[d] \\
 & \mathsf{ACA} \arrow[d] \arrow[dl] \\
\mathsf{RT}^2_2 \arrow[dr] & \mathsf{WKL} \arrow[d] \\
 & \mathsf{RCA}_0
\end{tikzcd}
$$

Presque tous les théorèmes sont empiriquement équivalents à un parmi cinq ensembles d'axiomes.

Exceptée la théorie de Ramsey...


ACA
RT22+WKL+RRT32
RT22
CAC+WKL
SRT22+COH
EM+ADS
PT22
RWKL[0']
POS+WWKL
FS(3)
CAC
P22
IPT22
SRAM
2-WWKL
ISig2+STS(2)
RRT32
FS(2)
WRT22
SCAC+CCAC
BSig2+COH+RRT22
EM
SRT22
ASRAM
DTCp
BSig2+2-RAN
2-POS
2-RAN
BSig2+Pi01G
TS(2)
SFS(2)
BSig2+RRT22
ADS
SCAC
EM+BSig2
D22
SEM+SADS
SIPT22
SPT22
ASRT22
ISig2+AMT
Pi01G
ISig2
STS(2)
RWWKL[0']
COH+WKL
SADS+CADS
CCAC
SADS
StCOH
SEM
1-GEN
AMT
RRT22
DNR[0']
wSRRT22
WKL
COH
BSig2
BSig2+CADS
BSig2+COH
CRT22+BSig2
StCRT22
StCADS
FIP
WWKL
PHPM
SRRT22
CRT22
RT1
PART
RWKL
nD2IP
1-POS
1-RAN
DNR
RCOLOR3
OPT
CADS
RWWKL
NCF
Kurtz
RCOLOR2
POS
AST
RCA

Comment prouver une non-implication ?

ω-structure $\mathcal{M} = \{\omega, \mathcal{S}, <, +, \cdot\}$

(i) ω est l'ensemble des entiers standards

(ii) $<$ est l'ordre naturel sur les entiers

(iii) $+$ et $\cdot$ sont les opérations standards sur les entiers

(iv) $\mathcal{S} \subseteq \mathcal{P}(\omega)$

Une ω-structure est déterminée par son second ordre $\mathcal{S}$.

Idéal de Turing $\mathcal{M}$

- $(\forall X \in \mathcal{M})(\forall Y \leq_T X)[Y \in \mathcal{M}]$
- $(\forall X, Y \in \mathcal{M})[X \oplus Y \in \mathcal{M}]$

Exemples

- $\{X : X$ est calculable $\}$
- $\{X : X \leq_T A \wedge X \leq_T B\}$ pour des ensembles A et B

Soit $\mathcal{M} = \{\omega, \mathcal{S}, <, +, \cdot\}$ une ω-structure

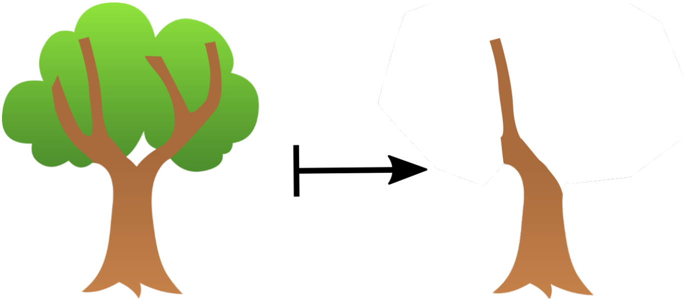
$$\mathcal{M} \models \mathsf{RCA}_0$$

$$\equiv$$

$\mathcal{S}$ est un idéal de Turing

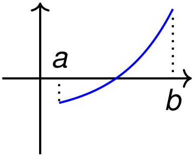
Certains théorèmes peuvent être vus comme des problèmes.

Lemme de König
Tout arbre infini à branchement fini admet un chemin infini.

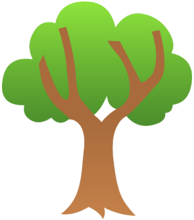


Certains théorèmes sont plus calculables que d'autres.

Théorème des valeurs intermédiaires
Pour toute fonction continue f sur un intervalle $[a, b]$ tel que $f(a) \cdot f(b) < 0$, il existe un réel $x \in [a, b]$ tel que $f(x) = 0$.



Lemme de König
Tout arbre infini à branchement fini admet un chemin infini.



Soit $\mathcal{M}$ un idéal de Turing et P, Q des problèmes.

Satisfaction

$$\mathcal{M} \models \mathsf{P}$$

si toute instance de P dans $\mathcal{M}$ a une solution dans $\mathcal{M}$.

Implication calculatoire

$$\mathsf{P} \models_c \mathsf{Q}$$

si tout idéal de Turing satisfaisant P satisfait Q.

Soient deux problèmes P et Q.

Comment prouver que $\mathsf{RCA}_0 + \mathsf{P} \nvdash \mathsf{Q}$?

Construire un idéal de Turing $\mathcal{M}$ tel que

- $\mathcal{M} \models \mathsf{P}$
- $\mathcal{M} \not\models \mathsf{Q}$

PROUVER QUE $\mathsf{RCA}_0 + \mathsf{P} \vdash \mathsf{Q}$

Choisir une instance I de Q sans solution calculable en I

Commencer avec $\mathcal{M}_0 = \{Z : Z \leq_T I\}$

Etant donné un idéal de Turing $\mathcal{M}_n = \{Z : Z \leq_T U\}$ pour un ensemble U,

Prouver que $\mathsf{RCA}_0 + \mathsf{P} \vdash \mathsf{Q}$

Choisir une instance I de Q sans solution calculable en I

Commencer avec $\mathcal{M}_0 = \{Z : Z \leq_T I\}$

Etant donné un idéal de Turing $\mathcal{M}_n = \{Z : Z \leq_T U\}$ pour un ensemble U,

1. choisir une instance $X \in \mathcal{M}_n$ de P

PROUVER QUE $\mathsf{RCA}_0 + \mathsf{P} \vdash \mathsf{Q}$

Choisir une instance I de Q sans solution calculable en I

Commencer avec $\mathcal{M}_0 = \{Z : Z \leq_T I\}$

Etant donné un idéal de Turing $\mathcal{M}_n = \{Z : Z \leq_T U\}$ pour un ensemble U,

1. choisir une instance $X \in \mathcal{M}_n$ de P
2. choisir une solution Y de X

PROUVER QUE $\mathsf{RCA}_0 + \mathsf{P} \vdash \mathsf{Q}$

Choisir une instance I de Q sans solution calculable en I

Commencer avec $\mathcal{M}_0 = \{Z : Z \leq_T I\}$

Etant donné un idéal de Turing $\mathcal{M}_n = \{Z : Z \leq_T U\}$ pour un ensemble U,

1. choisir une instance $X \in \mathcal{M}_n$ de P
2. choisir une solution Y de X
3. définir $\mathcal{M}_{n+1} = \{Z : Z \leq_T Y \oplus U\}$

Attention, ajouter des ensembles à $\mathcal{M}$,
risque d'ajouter des solutions à l'instance de Q !

Une propriété de faiblesse est une collection d'ensembles close par le bas par la réduction de Turing.

Exemples

- $\{X : X \text{ est low}\}$
- $\{X : A \not\leq_T X\}$ pour un ensemble A
- $\{X : X \text{ est hyperimmune-free}\}$

Soit une propriété de faiblesse $\mathcal{W}$.

Un problème P préserve $\mathcal{W}$ si pour tout $Z \in \mathcal{W}$, toute instance Z-calculable X de P admet une solution Y telle que $Y \oplus Z \in \mathcal{W}$

Lemma

Si P *préserve* $\mathcal{W}$ *et non* Q, *alors* $\mathsf{RCA}_0 + \mathsf{P} \nvdash \mathsf{Q}$

$$\begin{array}{c} \Pi^1_1\mathsf{CA} \\ \downarrow \\ \mathsf{ATR} \\ \downarrow \\ \mathsf{ACA} \\ \downarrow \\ \mathsf{WKL} \\ \downarrow \\ \mathsf{RCA}_0 \end{array}$$

LEMME FAIBLE DE KÖNIG

$2^{<\omega}$ est l'ensemble des chaînes binaires finies

Un arbre binaire est un ensemble $T \subseteq 2^{<\omega}$ clos par préfixes

Un chemin à travers T est une séquence infinie P telle que tous les segments initiaux sont dans T

WKL Tout arbre binaire infini admet un chemin infini.

$$\mathsf{RCA}_0 + \mathsf{WKL} \nvdash \mathsf{ACA}$$

(Jocksuch)

Soit $\mathcal{W}$ la collection des ensembles qui ne calculent pas le problème de l'arrêt

WKL préserve $\mathcal{W}$ contrairement à ACA

Questions ouvertes

$f : [\mathbb{N}]^{n+1} \to k$ est stable si pour tout $\sigma \in [\mathbb{N}]^n$, $\lim_y f(\sigma, y)$ existe.

SRT^n_k : RT^n_k restreint aux coloriages stables.

Un ensemble infini C est $\vec{R}$-cohésif for une séquence $R_0, R_1, \dots$ si pour tout i, soit $C \subseteq^* R_i$ soit $C \subseteq^* \overline{R_i}$.

COH : Toute collection d'ensembles a un ensemble cohésif.

$\emptyset'$-calculable | stable calculable

$$\mathsf{RT}^n_k \quad \Leftrightarrow \quad \mathsf{RT}^{n+1}_k$$

$\emptyset'$-calculable | stable calculable

$$\mathsf{RT}^n_k \quad \Leftrightarrow \quad \mathsf{RT}^{n+1}_k$$

"Tout ensemble Δ^0_2 a
un sous-ensemble ou
un sur-ensemble infini" $\Leftrightarrow$ SRT^2_2

$$\mathsf{RCA}_0 \vdash \mathsf{RT}^2_2 \leftrightarrow \mathsf{COH} \wedge \mathsf{SRT}^2_2.$$

Etant donné $f : [\mathbb{N}]^2 \to 2$, définir $\langle R_x : x \in \mathbb{N} \rangle$ par

$$R_x = \{y : f(x, y) = 1\}$$

Par COH, il existe un ensemble $\vec{R}$-cohésif C.

$f : [C]^2 \to 2$ est une instance de SRT^2_2

$$\mathsf{RCA}_0 \nvdash \mathsf{COH} \to \mathsf{SRT}^2_2$$

(Hirschfeldt, Jocksuch, Kjos-Hanssen, Lempp, and Slaman)

En préservant $\mathcal{W} = \{X :$
X ne calcule pas d'ensemble f-homogène $\}$
avec un forcing de Mathias calculable.

$$\mathsf{RCA}_0 \nvdash \mathsf{SRT}^2_2 \rightarrow \mathsf{COH}$$

(Chong, Slaman and Yang)

En utilisant un modèle non-standard contenant seulement des ensembles low.

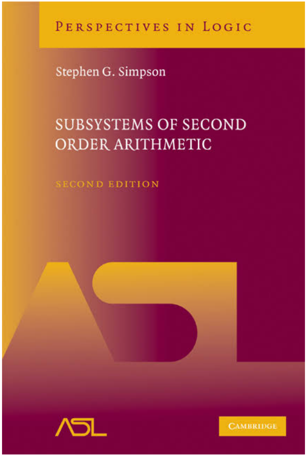
Questions dont la résolution peut apporter de nouvelles preuves plus élémentaires.

Théorème de Hindman : Pour tout k-coloriage des entiers, il existe un ensemble infini sur lequel les sommes finies sont monochromatiques.

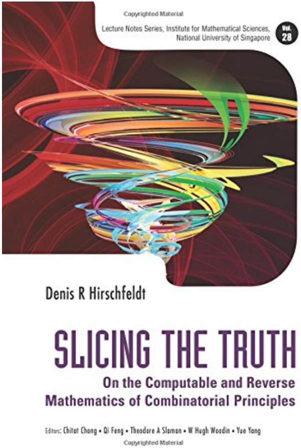
0	1	2	3	4
5	6	7	8	9
10	11	12	13	...

$$\left\{ \begin{array}{lll} 3 & 3+5 & 3+5+9 \\ 5 & 3+9 & \\ 9 & 5+9 & \end{array} \right\}$$

Quelle est la force exacte du théorème de Hindman ?



Subsystems of second-order arithmetic



Slicing the truth

RÉFÉRENCES

- David Hilbert and Paul Bernays.
  Grundlagen der Mathematik. I/Foundations of mathematics. I. Part A. Prefaces and §§1–2.
  College Publications, London, 2011.
- Stephen G. Simpson.
  Partial realizations of Hilbert's Program.
  J. Symbolic Logic, 53(2) :349–363, 1988.
- W. W. Tait.
  Finitism.
  Journal of Philosophy, 78(9) :524–546, 1981.